UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

ANDROSCOGGIN BANK and BRIDGEWATER CREDIT UNION, on behalf of themselves and all others similarly situated, Plaintiff, v. TARGET CORPORATION, Defendant.	Case No. 14-cv-1422 **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Comes now Plaintiffs Androscoggin Bank and Bridgewater Credit Union ("Plaintiffs"), acting individually and on behalf of all other persons similarly situated, and for their Complaint and demand for jury trial state and allege as follows:

INTRODUCTION

1. This case arises from one of the largest data breaches in history, in which criminals obtained sensitive financial and personal data from the accounts of up to 110 million Target Corporation ("Target," "Defendant," or "the Company") customers. Specifically, starting on or about November 27, 2013 and continuing until on or about December 15, 2013, unknown third parties obtained customer records, held by Target, of as many as 110 million individuals. Such data included customer names, credit and debit card numbers, the card expiration dates, card verification values (CVVs), PIN numbers, mailing addresses, phone numbers, and email addresses.

2. As alleged herein, this data breach was made possible only because Target – the second largest retailer in the nation – failed to maintain adequate security

protocols despite having suffered two nearly identical data breaches in the preceding years and being warned multiple times – once in April of 2013 and again in August of 2013 – of the *precise* threat that led to the ultimate compromise.

3. As details of the data breach emerged, security experts professed bewilderment by the level of negligence exhibited by Defendant in maintaining the security of highly sensitive consumer financial data. Reports proliferate of Target's "astonishingly" vulnerable security systems, which "lack[] the virtual walls and motion detectors found [as a matter of course] in secure networks."[1]

4. In an effort to prevent a mass exodus of customers, Target CEO Gregg Steinhafel (who resigned on May 5, 2014) took pains to assure consumers that "they will not be held financially responsible for any credit and debit card fraud."[2] Notably absent from that statement, however, is the fact that it is the nation's financial institutions – and not Target – ensuring that this is the case. To date, Plaintiffs, along with all other financial institutions making up the proposed Class, have incurred significant costs associated with protecting their customers' accounts, particularly in the form of providing notice to customers, reissuing payment cards, and refunding fraudulent charges associated with bank accounts of customers who used their cards at Target during the period of the latest data breach. A recent study conducted by the Consumer Bankers

[1] Elizabeth A. Harris, Nicole Perlroth, Nathaniel Popper and Hilary Stout. "A Sneaky Path into Target Customers' Wallets." N.Y. Times (Jan. 17, 2014) (*available at* http://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.html).

[2] "A Message From CEO Gregg Steinhafel About Target's Payment Card Issues." (Dec. 20, 2013) (*available at* http://pressroom.target.com/news/a-message-from-ceo-gregg-steinhafel-about-targets-payment-card-issues).

Association and the Credit Union National Association estimates the costs of card replacements, alone, to ultimately rest around $200 million.[3] This figure does not, however, include costs associated with reimbursing customers for fraudulent charges, or costs associated with lost transactional opportunities arising from decreasing consumer confidence in the security of payment cards.

5. Plaintiffs bring this class action on behalf of all financial institutions – including banks and credit unions – in the United States who suffered injury as a result of a security breach compromising Target store customers' names, credit and debit card numbers, card expiration dates, person identification numbers ("PINs"), and card verification values (hereinafter the "Target Data Breach"), forcing these institutions to (a) cancel or reissue any access device affected by the Target Data Breach; (b) close any deposit, transaction, or other accounts affected by the breach, including but not limited to stopping payments or blocking transactions with respect to the accounts; (c) open or reopen any deposit, transaction, or other accounts affected by the Target Data Breach; (d) refund or credit any cardholder to cover the cost of any unauthorized transaction relating to the Target Data Breach; or (e) notify cardholders affected by the Target Data Breach.

PARTIES

6. Plaintiff Androscoggin Bank ("Androscoggin") is a community bank headquartered in Lewiston, Maine. Androscoggin was chartered in 1870 and provides

[3] Juan Carlos Rodriguez, "Target Hack Costs Over $200M for Banks, Groups Say." Law360 (Feb. 20, 2014) (available at http://www.law360.com/privacy/articles/511396?nl_pk=9e2e8a6f-f702-466f-84ee-2a41d5618600&utm_source=newsletter&utm_medium=email&utm_campaign=privacy).

banking services for both individual and business customers throughout Maine. Androscoggin's customers had their personal and financial information stolen as a result of a massive data breach occurring throughout the country at the stores of Defendant Target Corporation, from approximately November 27, 2013, until December 15, 2013. As a result of this theft, Androscoggin experienced losses, including, without limitation, the cost of notifying customers and reissuing debit cards in order to prevent future fraudulent activity, as well as refunding fraudulent charges associated with customer accounts affected by Target's data breach.

7. Plaintiff Bridgewater Credit Union ("Bridgewater") is a state-chartered credit community union headquartered in Bridgewater, Massachusetts. Bridgewater is a member-owned credit union and a full service financial institution offering a variety of savings and loan products to anyone living and working or having business within Barstable, Bristol, Norfolk, or Plymouth Counties in Massachusetts. Bridgewater's customers had their personal and financial information stolen as a result of a massive data breach occurring throughout the country at the stores of Defendant Target Corporation, from approximately November 27, 2013, until December 15, 2013. As a result of this theft, Bridgewater experienced losses, including, without limitation, the cost of notifying customers and reissuing debit cards in order to prevent future fraudulent activity, as well as refunding fraudulent charges associated with customer accounts affected by Target's data breach.

8. Defendant Target Corporation is a corporation, incorporated under the laws of Minnesota and headquartered in Minneapolis, Minnesota.

JURISDICTION AND VENUE

9. The Court has subject matter jurisdiction over this class action pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5,000,000.00, exclusive of interest and costs, and is a class action in which some Members of the Class are citizens of states different than Defendant. *See* 28 U.S.C. § 1332(d)(2)(A).

10. Venue properly lies in this district pursuant to 28 U.S.C. § 1391. Defendant maintains its principal place of business in this District, Defendant regularly transacts business in this District, and many of the acts and transactions giving rise to this action occurred in this District.

GENERAL ALLEGATIONS

11. Target is an American discount retailer or "superstore," selling a wide array of consumer merchandise such as clothing, home furnishings, foodstuffs, electronics, books, toys, and pharmaceuticals. It is the second-largest discount retailer in the United States – behind Walmart – with 1,797 locations spread across the country.

12. On December 18, 2013, security researcher and blogger Brian Krebs reportedthat Target was investigating a massive data breach, in which unknown third parties illegally obtained information related to Target customers' credit and debit cards,

including the customers' names, credit/debit card number, the card's expiration date, and the card's CVV.[4]

13. According to Krebs, the data breach began on November 27, 2013 – also known as "Black Friday," typically the busiest shopping day of the year in the United States – and continued until at least December 15, 2013.

14. According to Krebs, Target became aware of the breach at some point during this period. However, at *no point* prior to Krebs' article did the Company take *any* steps to alert its customers, or their financial institutions, that their critically sensitive financial information was in the hands of thieves.

15. Following Mr. Krebs' announcement, on December 19, 2013, Target issued a statement confirming that a security breach occurred and asserted that 40 million credit and debit card accounts may have been impacted between November 27, 2013, and December 15, 2013. *See* "Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores," *available at* http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores (hereinafter "December 19, 2013, Press Release")

16. Not until December 20, 3013, over three weeks after the data breach began, did Target reach out to its impacted customers to inform them of the issue. *See* December 20, 2013, Target Email to Customers, *available at*

[4] Brian Krebs, "Sources: Target Investigating Data Breach," *Krebs on Security* (Dec. 18, 2013) (*available at* http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/).

https://corporate.target.com/discover/article/Important-Notice-Unauthorized-access-to-payment-ca.

17. In the December 20, 2013, Target Email to Customers, Target admitted that the security breach "included customer name, credit or debit card number, and the cards's expiration date and CVV."

18. Target further acknowledged that "encrypted debit card PIN data was among the information stolen when its systems were breached during the peak holiday shopping period." Target noted that "its investigation now show that encrypted PIN data was 'removed' from its systems." *See* "Target Says Encrypted PIN Data Taken in Breach," THE WALL STREET JOURNAL, Dec. 27, 2013 *available at* http://online.wsj.com/news/articles/SB10001424052702303345104579284440022934198?cb=logged0.0365547111723572.

19. On January 10, 2014, Target made another announcement, this time conceding that its "investigation has determined that the stolen information includes names, mailing addresses, phone numbers or email addresses for up to 70 milllion individuals." *See* "Target Provides Update on Data Breach and Financial Performance," *available at* http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance (hereinafter "January 10, 2014, Target Press Release")

20. Reports have show that the information for the 70 million individuals was stored separately from the 40 million credit and debit card accounts that Target previously admitted was impacted. *See* "Target Now Says 70 Million People Hit in Data Breach," THE WALL STREET JOURNAL, Jan. 10, 2014, *available at*

http://online.wsj.com/news/articles/SB10001424052702303754404579312232546392464

.

21. In combination with the initially reported 40 million customers whose credit and debit card accounts were affected, the Target data breach impacted approximately up to 110 million consumers.

22. Not only do thieves have the stolen information, but they are also actively selling this data on the black market, for purposes of identity theft and bank fraud. In a follow up to his initial story, Brian Krebs documented a search of a black market credit and debit card data brokerage site, in which cards stolen from the data breach were being bought and sold:

> [M]y source at the big bank had said all of the cards his team purchased from this card shop that matched Target's Nov. 27 – Dec. 15 breach window bore the base name Tortuga, which is Spanish for "tortoise" or "turtle."
>
> Indeed, shortly after the Target breach began, the proprietor of this card shop — a miscreant nicknamed "Rescator" and a key figure on a Russian-language cybercrime forum known as "Lampeduza" — was advertising a brand new base of one million cards, called Tortuga.
>
> Rescator even…advertis[ed a] "valid 100% rate," and offer[ed] a money-back guarantee on any cards from this "fresh" base that were found to have been canceled by the card issuer immediately after purchase. In addition, sometime in December, this shop ceased selling cards from other bases aside from those from the Tortuga base. As the month wore on, new Tortuga bases would be added to shop, with each base incrementing by one with almost every passing day (e.g., Tortuga1, Tortuga2, Tortuga3, etc.).

> Another fascinating feature of this card shop is that *it appears to include the ZIP code and city of the store from which the cards were stolen*. One fraud expert I spoke with who asked to remain anonymous said this information is included to help fraudsters purchasing the dumps make same-state purchases, thus avoiding any knee-jerk fraud defenses in which a financial institution might block transactions out-of-state from a known compromised card.[5]

23. While Target offers a vague assurance that it has "identified and resolved the issue," in the same statement the Company directs readers to anti-fraud websites of the FTC, credit reporting bureaus, and state Attorney Generals' offices.[6]

24. Further, despite the Company's unconvincing statements on the issue, it is still unknown how such a systemic, cataclysmic act of theft could be perpetuated. While some reports suggest that the thieves placed small chips into the credit card readers at the Company's checkout lanes – a criminal act commonly referred to as "skimming" – other researchers note the improbability of such a massively coordinated effort (again, Target's stores number almost 1,800, nationwide), and instead suggest either malicious software or even an organized effort from within the Company.[7]

DEFENDANT'S CONDUCT HAS HARMED PLAINTIFFS AND CLASS MEMBERS

[5] Brian Krebs, "Cards Stolen in Target Breach Flood Underground Markets." *Krebs on Security*. (Dec. 20, 2013) (*available at* http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/).

[6] Target, "A Message From CEO Gregg Steinhafel About Target's Payment Card Issues." (Dec. 20, 2013) (*available at* https://corporate.target.com/discover/article/important-notice-unauthorized-access-to-payment-ca).

[7] Antone Gonsalves, "Target Breach Likely Involved Inside Knowledge, Experts Say." *PC World* (Dec. 21, 2013) (*available at* http://www.pcworld.com/article/2082268/target-breach-likely-involved-inside-knowledge-experts-say.html).

25. Plaintiffs maintain and administer the accounts of customers that include persons and/or entities that made purchases at Target stores during the period of November 27, 2013, to December 15, 2013, using debit cards issued by Plaintiffs. Accordingly, the sensitive financial data of Plaintiff's customers, including names, card numbers, card expiration dates, card CVVs, and in certain instances customer PINs, have been obtained by thieves.

26. But for Defendants' negligence, thieves could not have accessed this information – either via "skimming" from Target's point-of-sale machines, installing some type of malicious software in the Company's infrastructure, or utilizing Company insiders to otherwise obtain these data.

27. Target failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach described in this Complaint, despite being on notice that its security protocols were especially vulnerable to cyber-attack.

28. In fact, at the time of the data breach occurring on or about November 27, 2013, and continuing to on or about December 15, 2013, Target had been put on notice by two previous data breaches and two explicit warnings from Visa, all indicating that Target's networks and POS machines were at risk of cyber-attack.

29. The first data breach was revealed after the criminal trial of a hacker who stole payment card information from Heartland Payment Systems from 2005-2007. Further, in 2011, Target informed its customers that their names and and email addresses had been exposed in a data breach suffered by Epsilon, a marking firm hired by Target.

Moreover, throughout 2013, Target received numerous warnings from Visa about malware installations in POS payment machines.

30. As a result of Target's noncompliance with standards mandated both by industry and state statutes, the sensitive financial data of Plaintiff's and Class Members' customers – including names, card numbers, card expiration dates, card CVVs, and in certain instances customer PINs – are not only in the hands of thieves, but are brazenly being trafficked on black market websites.

31. Accordingly, and as a result of Defendant's conduct, Plaintiffs and Class Members experienced losses in the form of reissuing payment cards and refunding fraudulent charges for customer accounts affected by Target's data breach, as well as costs associated with notifying customers. These costs and expenses will continue to accrue as additional fraud alerts and fraudulent charges are discovered.

CLASS ALLEGATIONS

32. Plaintiffs bring this action, pursuant to Rule 23 of the Federal Rules of Civil Procedures, individually and on behalf of all Members of the following classes (collectively referred to as "the Class" or "Class"):

> **National Class:** All financial institutions – including banks and credit unions – in the United States that have had the confidential financial data associated with their customers' accounts – including but not limited to customer names, card numbers, card expiration dates, card CVVs, and in certain instances customer PINs – compromised as a result of the data breach at Target stores from the period beginning on or about November 27, 2013 and ending on or about December 15, 2013.

> **Maine Sub-Class:** All financial institutions – including banks and credit unions – in the State of Maine that have had the confidential financial data associated with their customers' accounts – including but not limited to customer names, card numbers, card expiration dates, card CVVs, and in certain instances customer PINs – compromised as a result of the data breach at Target stores from the period beginning on or about November 27, 2013 and ending on or about December 15, 2013.
>
> **Massachusetts Sub-Class:** All financial institutions – including banks and credit unions – in the Commonwealth of Massachusetts that have had the confidential financial data associated with their customers' accounts – including but not limited to customer names, card numbers, card expiration dates, card CVVs, and in certain instances customer PINs – compromised as a result of the data breach at Target stores from the period beginning on or about November 27, 2013 and ending on or about December 15, 2013.

33. Excluded from the Class are the following individuals and/or entities: Target and its parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Target has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family Members.

34. Plaintiffs reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

35. The Class is so numerous that joinder of all Members is impracticable. The number of separate individuals whose private financial data have been compromised as a result of the data breach described herein number at approximately 110 million, making the number of affected financial institutions – all of whom are members of the proposed Class – number in at least the thousands.

36. There are questions of law or fact common to the Class. These questions include, but are not limited to, the following:

a. Whether Defendant failed to provide adequate security and/or protection for its computer systems containing customers' financial and personal data;

b. Whether the conduct of Defendant resulted in the unauthorized breach of its computer systems containing customers' financial and personal data;

c. Whether Defendant improperly retained customer personal and financial information despite representations that it would not keep such information;

d. Whether Defendant disclosed, either directly or indirectly, the private financial information of customers;

e. Whether Defendant violated Minn. Stat. § 325E.64; Minn. Stat. § 325.43; Mass. Gen. Laws Ch. 93A; and Me. Rev. Stat. Ann. Tit. 5 § 207;

f. Whether Plaintiff and members of the Class have been injured by Defendant's violations of Minnesota law, Massachusetts law and/or Maine law;

g. Whether Plaintiff and members of the Class are entitled to injunctive relief; and

h. Whether Plaintiff and Members of the Class are entitled to damages and the measure of such damages.

37. Plaintiffs' claims are typical of the claims of the Class in that Plaintiffs and Class Members experienced losses, as a result of Defendant's conduct, in the form of reissuing debit cards and refunding fraudulent charges for accounts affected by Target's data breach, as well as incurring costs for the notification of its customers.

38. Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs' interests do not conflict with the interests of the Class Members. Furthermore, Plaintiffs have retained competent counsel experienced in class action litigation. Plaintiffs' counsel will fairly and adequately protect and represent the interests of the Class.

39. Plaintiffs assert that pursuant to Fed. R. Civ. P. 23(b)(3), questions of law or fact common to the Class Members predominate over any questions affecting only individual Members.

40. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Even if Class Members themselves could afford such individual litigation, given the complex legal and factual issues involved, and

considering that the Class consists of thousands of financial institutions, individualized litigation would significantly increase the delay and expense to all parties and to the Court. Individualized litigation would also create the potential for inconsistent or contradictory rulings. By contrast, a class action presents far fewer management difficulties, allows claims to be heard which may otherwise go unheard because of the relative expense of bringing individual lawsuits, and provides the benefits of adjudication, economies of scale and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT ONE
(Violation of Minn. Stat. § 325E.64)
(Brought on behalf of the Class)

41. Plaintiffs adopt and incorporate each and every allegation of this complaint as if stated fully herein.

42. The Minnesota Legislature, in an effort to combat cybercrime and to protect financial institutions from negligent practices of retailers, enacted Minn. Stat. § 325E.64, which states in pertinent part:

> No person or entity conducting business in Minnesota that accepts an access device in connection with a transaction shall retain the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction. A person or entity is in violation of this section if its service provider retains such data subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction.

43. Plaintiffs and Class Members are "financial institutions" within the meaning of Minn. Stat. § 325E.64.

44. As alleged in this Complaint, Defendant violated the above-quoted provisions of Minn. Stat. § 325E.64, at minimum, when it retained Plaintiffs' and Class Members' customers' card security code data, PIN verification code numbers, and/or the full contents of any track of magnetic stripe data, subsequent to the authorization of the customers' transactions. Further, in the case of a PIN debit transaction, Target violated Minn. Stat. § 325E.64 when it held such data subsequent to 48 hours after authorization of the customers' transactions.

45. Accordingly, pursuant to Minn. Stat. § 325E.64, Plaintiffs and Class Members are entitled to reimbursement from Defendant for "the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders."

COUNT TWO
(Violation of Minn. Stat. § 325D.43, *et seq.*)
(Brought on behalf of the Class)

46. Plaintiff adopts and incorporates each and every allegation of this complaint as if stated fully herein.

47. Defendant's conduct as alleged herein constitutes a deceptive business practice as proscribed by the Minnesota Uniform Deceptive Trade Practices Act, Minn. Stat. § 325D.43, *et seq.*

48. Pursuant to Minn. Stat. § 325D.44, a corporation violates the Minnesota Uniform Deceptive Trade Practices Act when it "represents that . . . services have . . .

characteristics . . . that they do not have," or "engages in any other conduct which similarly creates a likelihood of confusion or of misunderstanding." Minn. Stat. § 325D.44, subd 1(5) & (13).

49. When Defendant represented to its customers that it would adhere to certain, minimal security standards, and when Defendant did not, in fact, adhere to those security standards, Defendant violated the Uniform Deceptive Practices Act.

50. Plaintiffs and Class Members seek an order to enjoin Defendant from such deceptive practices, to restore to Plaintiffs and Class Members their interest in money or property that may have been acquired by Defendant by means of its deceptive practices, and costs and attorneys' fees.

COUNT THREE
(Negligence)
(Brought on behalf of the Class)

51. Plaintiffs adopt and incorporate each and every allegation of this complaint as if stated fully herein.

52. Defendant owed Plaintiffs and Class Members a duty to exercise reasonable care in the acquisition, maintenance, and storage of their customers' financial information, including names, card numbers, card expiration dates, card CVVs, and customer PINs. Such duty includes the implementation of security infrastructure and protocols.

53. Defendant also owed Plaintiffs and Class Members a duty to timely disclose the nature and extent of the data breach extending from November 27, 2013, to December 15, 2013.

54. As alleged herein, Defendant breached its duty to Plaintiffs and Class Members where it failed to exercise reasonable care by maintaining adequate security infrastructure and protocols, thereby failing to safeguard Plaintiffs' and Class Members' customers' financial information.

55. As alleged herein, Defendant breached its duty to Plaintiffs and Class Members where it failed to timely alert affected consumers to the existence – as well as the depth and breadth – of the data breach extending from November 27, 2013, to December 15, 2013.

56. Defendant's breach of duty proximately caused injury to Plaintiffs and Class Members, including losses in the form of reissuing debit cards and refunding fraudulent charges for accounts affected by Target's data breach, as well as incurring costs for the notification of its customers.

57. Plaintiffs seek an award of actual damages individually and on behalf of the Class.

COUNT FOUR
(Violation of Mass. Gen. Laws Ch. 93A)
(Brought on behalf of the Massachusetts Sub-Class)

58. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs of this Complaint, as though fully set forth here.

59. The conduct of Defendant, as hereinabove alleged constitutes unfair and deceptive acts or practices within the meaning of Mass. Gen Law. Ch. 93A, § 2.

60. Plaintiffs and Class Members have been damaged as the result of Defendants' breach of contract, including, but not limited to, incurring losses in the form

of reissuing debit cards, refunding fraudulent charges to accounts affected by Target's data breach and costs for the notification of its customers.

COUNT FIVE
(Violation of Me. Rev. Stat. Ann. Tit. 5 § 207)
(Brought on behalf of the Maine Sub-Class)

61. Plaintiffs reallege and incorporate by reference the allegations contained in the preceding paragraphs of this Complaint, as though fully set forth here.

62. The conduct of Defendant, as hereinabove alleged constitutes unfair and deceptive acts or practices within the meaning of Me. Rev. Stat. Ann. Tit. 5 § 207.

63. Pursuant to Me. Rev. Stat. Ann. Tit. 5 § 213, Plaintiffs suffered loss of money as a result of Defendant's unlawful practices and therefore they seek damages, restitution and such other equitable relief as the Court determines to be necessary and proper.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38, Plaintiff, individually and on behalf of the Class it seeks to represent, demands a jury on any issue so triable of right by a jury.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of itself and all Class Members, request judgment be entered against Defendant and that the Court grant the following:

1. An order determining that this action may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, that Plaintiffs are proper class representatives, that Plaintiffs' attorneys be appointed Class counsel pursuant to Rule 23(g) of the Federal Rules of Civil Procedure, and that Class notice be promptly issued;

2. Judgment against Defendant for Plaintiffs' and Class Members' asserted causes of action;

3. Appropriate declaratory relief against Defendant;

4. Preliminary and permanent injunctive relief against Defendant;

5. Equitable relief in the form of restitution and disgorgement of revenues wrongfully obtained as a result of Defendant's wrongful conduct;

6. An award of actual damages and compensatory damages in an amount to be determined;

7. An award of punitive damages;

8. An award of reasonable attorney's fees and other litigation costs reasonably incurred; and

9. Any and all relief to which Plaintiffs and the Class may be entitled.

DATED: May 7, 2014

Respectfully Submitted,

By: /s/ Karen H. Riebel

Karen Hanson Riebel, #219770
Robert K. Shelquist, #21310X
Gregg M. Fishbein, #202009
Kate M. Baxter-Kauf, #392037
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South
Suite 2200
Minneapolis, MN 55401
Telephone: 612-596-4097
Facsimile: 612-339-0981
khriebel@locklaw.com
rkshelquist@locklaw.com
gmfishbein@locklaw.com
kmbaxter-kauf@locklaw.com

Andrew N. Friedman
Douglas J. McNamara
Mary J. Bortscheller

COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Avenue, N.W.
Suite 500, West Tower
Washington, DC 20005
Telephone: (202) 408-4600
Facsimile: (202) 408-4699
afriedman@cohenmilstein.com
dmcnamara@cohenmilstein.com
mbortscheller@cohenmilstein.com

Attorneys for Plaintiffs Androscoggin Bank and Bridgewater Credit Union